Hyper-atoms and the Kemperman's critical pair Theory

Yahya O. Hamidoune[*]

August, 15-2007

Abstract

In the present work, we introduce the notion of a hyper-atom and prove their main structure theorem. We then apply the global isoperimetric methodology to give a new proof for Kemperman's structure Theory and a slight improvement.

1 Introduction

A basic tool in Additive Number Theory is the following generalization of the Cauchy-Davenport Theorem [2, 3] due to Kneser:

Theorem 1 (Kneser [19, 21]) *Let G be an abelian group and let $A, B \subset G$ be finite subsets of G. Then $|A+B| \geq |A+H| + |B+H| - |H|$, where H is the period of $A+B$.*

The description for the subsets with $|A+B| = |A| + |B| - 1$ needs some terminology:

A decomposition $A = A_0 \cup A_1$ is said to be a H*–quasi-periodic decomposition* if $A_0 + H = A_0$ and A_1 is contained in some H–coset. Let $A, B \subset G$.

A pair $\{A, B\}$ will be called an *elementary pair* if one of the following conditions holds:

(SP1) there is $d \in G$, with order $\geq |A|+|B|-1$ such that A and B are arithmetic progressions with difference d,

(SP2) $\min(|A|, |B|) = 1$,

(SP3) A is aperiodic and there is a finite subgroup H and $g \in G$ such that A, B are contained in some H–cosets and $g - B = H \setminus A$, and for all c, $|(c-A) \cap B| \neq 1$,

(SP4) there is a subgroup H with a prime order such that A, B are contained in some H-cosets and $|A|+|B| = |H|+1$, and moreover there is a unique $c \in G$ such that $|(c-A) \cap B| = 1$.

An elementary pair satisfying one of the conditions (SP1), (SP2) or (SP3) will be called a *strict elementary pair*.

[*] Université Pierre et Marie Curie, Paris hamidoune@math.jussieu.fr

Notice that the condition "with a prime order" in SP4 is not present in Kemperman's formulation. Hence the class of elementary pairs in the sense of Kemperman is larger than our class. This will produce a slightly more precise result than the result proved by Kemerman:

Theorem 2 *[17] Let A, B be finite subsets of an abelian group G with $|G| \geq 2$.*

Then the following conditions are equivalent:

- *(I) $|A+B| = |A|+|B|-1$, and moreover $|(c-A)\cap B| = 1$ for some c if $A+B$ is periodic.*
- *(II) There is a nonzero subgroup H and H-quasi-periodic decompositions $A = A_0 \cup A_1$ and $B = B_0 \cup B_1$ such that (A_1, B_1) is an elementary pair and $|(\phi(a_1+b_1)-\phi(A))\cap\phi(B)| = 1$, where $\phi : G \mapsto G/H$ is the canonical morphism and $a_1 \in A_1$ and $b_1 \in B_1$.*

The redundant condition $|\phi(A+B)| = |\phi(A)|+|\phi(B)|-1$ present in Kemperman's formulation was omitted since it is a consequence of the condition "$|(\phi(a_1+b_1)-\phi(A))\cap\phi(B)| = 1$" by Scherck's Theorem 4. The original and unique previously known proof of Kemperman's result uses the additive local transformations introduced by Cauchy and Davenport [2, 3].

Recently the author introduced the isoperimetric method allowing to derive additive inequalities from global properties of the fragments and atoms (subsets where the objective function $|A+B|-|A|$ achieves its non trivial minimal value).

This method can be applied to abstract graphs and non abelian groups and have implications that could not be derived using the local transformations. However in the abelian case, it was not clear how to derive the Kneser-Kemperman Theory using this method.

Very recently Balandraud introduced some isoperimetric objects and proposed a proof, requiring several pages, of Kneser's Theorem using as a first step our result that the 1-atom containing 0 is a subgroup.

On the other side, alternative proofs for results proved first using the isoperimetric method, based on Kemperman's Theory as a main tool, were obtained by Grynkiewicz in [5] and Lev [18].

In the present work, we introduce the notion of a hyper-atom and prove the main structure theorem for hyper-atoms. We then apply the global isoperimetric methodology introduced in [14] to give a new proof for Kemperman's structure Theory with a slight improvement. The methods introduced in the present work allow quite likely much more complicated descriptions for subsets A, B with $|A+B| = |A|+|B|+m$, with small some small values of $m \geq 0$. We made the calculations for $m = 0$, obtaining a new proof of a recent result due Grynkiewicz in [6], that extends to all abelian groups a result proved by Rødseth and the author [16]. However we shall limit ourselves to Kemperman's Theory in order to illustrate the method in a relatively simple context.

2 Terminology and preliminaries

Let A, B be subsets of G. The subgroup generated by A will be denoted by $\langle A\rangle$. The *Minkowski sum* is defined as

$$A+B=\{x+y\ :\ x\in A \text{ and } y\in B\}.$$

Let H be a subgroup. A partition $A=\bigcup\limits_{i\in I} A_i$, where A_i is the nonempty intersection of some H–coset with A will be called a *H–decomposition* of A.

For an element $x\in G$, we write $r_{A,B}(x)=|(x-B)\cap A|$. Notice that $r_{A,B}(x)$ is the number of distinct representations of x as a sum of an element of A and an element of B.

We use the following well known and easy fact:

Lemma 3 *[19] Let G be a finite group and let A, B be subsets such that $|A|+|B|\ge |G|+t$. Then $r_{A,B}(x)\ge t$.*

We shall use the following result:

Theorem 4 *(Scherk)[20]. Let X and Y be nonempty finite subsets of an abelian group G. If there is an element c of G such that $|X\cap(c-Y)|=1$, then $|X+Y|\ge |X|+|Y|-1$.*

Scherck's Theorem follows easily from Kneser's Theorem, c.f. [4]. We give in the appendix a short direct proof for this result.

We need Vosper's Theorem:

Theorem 5 *Let A, B be subsets of a group G with a prime order such that $|A|,|B|\ge 2$ and $|A+B|=|A|+|B|-1\le |G|-2$. Then A, B are arithmetic progressions with the same difference.*

As showed in [11, 13], this result follows in few lines from the intersection property of the 2–atoms.

Let V be a set and let $E\subset V\times V$. The relation $\Gamma=(V,E)$ will be called a *graph.* The elements of V will be called *points.* The graph Γ is said to be *reflexive* if $(x,x)\in E$, for all x. We shall write

$$\partial(X)=\Gamma(X)\setminus X.$$

Let $\Gamma=(V,E)$ be a locally finite graph with $|V|\ge 2k-1$. The *kth–connectivity* of Γ is

$$\kappa_k(\Gamma)=\min\{|\partial(X)|\ :\ \ \infty>|X|\ge k \text{ and } |X\cup\Gamma(X)|\le |V|-k\},$$

where $\min\emptyset=|V|-2k+1$.

Let G be a group, written additively, and let S be a subset of G. The graph (G,E), where $E=\{(x,y): -x+y\ \in S\}$ is called a *Cayley graph.* It will be denoted by $\mathrm{Cay}(G,S)$.

Let $\Gamma = \mathrm{Cay}(G, S)$ and let $F \subset G$. Clearly $\Gamma(F) = F + S$.

A general formalism, including the most recent isoperimetric terminology may be found in a the recent paper [13].

We recall that Menger's Theorem which is a basic min-max relation from Graph Theory [14, 19, 21] has several implications in number Theory. We need the following consequence of Menger's Theorem:

Proposition 6 *[14] Let Γ be a locally finite reflexive graph and let k be a nonnegative integer with $k \leq \kappa_1$. Let X a finite subset of V such that* $\min(|V| - |X|, |X|) \geq k$. *There are pairwise distinct elements $x_1, x_2, \cdots, x_k \in X$ and pairwise distinct elements $y_1, y_2, \cdots, y_k \notin X$ such that*

- $(x_1, y_1), \cdots, (x_k, y_k) \in E$,
- $|X \cup \{y_1, \cdots, y_k\}| = |X| + k$,

We call the property given in Proposition 6 the *strong isoperimetric property.*

3 Isoperimetric tools

The isoperimetric method is usually developed in the context of graphs. We need in the present work only the special case of Cayley graphs on abelian groups that we shall identify with group's subsets.

Throughout all this section, S denotes a finite generating subset of an abelian group G, with $0 \in S$.

For a subset X, we put $\partial_S(X) = (X + S) \setminus X$ and $X^S = G \setminus (X + S)$. We need the following lemma:

Lemma 7 *[1, 13]Let X be a subset of G. Then $(X^S)^{-S} + S = X + S$.*

The last lemma is proved in Balandraud [1] and generalized in [13].

We shall say that a subset X induces a *k–separation* if $|X| \geq k$ and $|X^S| \geq k$. We shall say that S is k–separable if some X induces a k–separation.

Suppose that $|G| \geq 2k - 1$. The *kth–connectivity* of S is defined as $\kappa_k(S) = \kappa_k(\mathrm{Cay}(G, S))$. By the definition we have

$$\kappa_k(\Gamma) = \min\{|\partial(X)| \ : \ \infty > |X| \geq k \text{ and } |X + S| \leq |G| - k\},$$

where $\min \emptyset = |G| - 2k + 1$.

A finite subset X of G such that $|X| \geq k$, $|G \setminus (X + S)| \geq k$ and $|\partial(X)| = \kappa_k(S)$ is called a *k–fragment* of S. A k–fragment with minimum cardinality is called a *k–atom.*

Let S be a non–k–separable subset such that $|G| \geq 2k-1$. Then G is necessarily finite. In this case, a *k–fragment* (resp. *k–atom*) is a set with cardinality k.

These notions, are particular cases some concepts in [7, 10, 11, 12, 13]. The reader may find all basic facts from the isoperimetric method in the recent paper [13].

A k–fragment of $-S$ will be called a *negative* k–fragment.

Notice that $\kappa_k(S)$ is the maximal integer j such that for every finite subset $X \subset G$ with $|X| \geq k$,

$$|X+S| \geq \min\Big(|G|-k+1, |X|+j\Big). \tag{1}$$

Formulae (1) is an immediate consequence of the definitions. We shall call (1) the *isoperimetric inequality.* The reader may use the conclusion of this lemma as a definition of $\kappa_k(S)$. The following upper bound follows by the inequality $|\partial(\{0\})| \geq \kappa_1$:

$$\kappa_1(S) \leq |S|-1. \tag{2}$$

The basic intersection theorem is the following:

Theorem 8 *[11, 13] Assume $|G| \geq 2k-1$. Let A be a k–atom and let F be a k-fragment such that $|A \cap F| \geq k$. Then $A \subset F$. In particular distinct k-atoms intersect in at most $k-1$ elements.*

The structure of 1–atoms is the following:

Proposition 9 *[9, 8]*

Let S be a generating subset of an abelian group G with $0 \in S$. Let H be a 1–atom of S with $0 \in H$. Then H is a subgroup. Moreover

$$\kappa_1(S) \geq \frac{|S|}{2}, \tag{3}$$

Proof. Take $x \in H$. Since $x \in (H+x) \cap H$ and since $H+x$ is a 1–atom, we have $H+x = H$ by Theorem 8. Therefore H is a subgroup. Since S generates G, we have $|H+S| \geq 2|H|$, and hence $\kappa_1(S) = |H+S| - |H| \geq \frac{|S+H|}{2} \geq \frac{|S|}{2}$. ∎

Let us mention the following relation between 1–fragments and 2–fragments. We note that a similar relation holds for non abelian groups and even for abstract graphs.

Lemma 10 *Let S be a finite generating 2–separable subset of an abelian group G with $0 \in S$ and $\kappa_2(S) \leq |S|-1$. Then $\kappa_2 = \kappa_1$. Moreover every 2–fragment is a 1–fragment. Also every 1–fragment F, with $2 \leq |F| \leq |G|-|S|-1$ is a 2–fragment.*

Lemma 10 follows immediately by the definitions.

The next result is proved in [10]. The finite case is reported with almost the same proof in [12].

Theorem 11 *[10, 12] Let S be a finite generating 2–separable subset of an abelian group G with $0 \in S$ and $\kappa_2(S) \leq |S|-1$. Let H be a 2–atom with $0 \in H$. Then H is a subgroup or $|H| = 2$.*

The next result is an immediate consequence of [[10], Theorem 4.6]. The finite case (used to solve Lewin's conjectures on the Frobenius number) is reported with almost the same proof in [12].

Corollary 12 *[[10],Theorem 4.6] Let S be a 2–separable finite subset of an abelian group G such that $0 \in S$, $|S| \leq (|G|+1)/2$ and $\kappa_2(S) \leq |S|-1$.*

If S is not an arithmetic progression then there is a subgroup H which is a 2–fragment of S.

Proof.

Suppose that S is not an arithmetic progression.

Let H be a 2- atom such that $0 \in H$. If $\kappa_2 \leq |S|-2$, then by Lemma 10 $\kappa_2 = \kappa_1$ and H is also a 1–atom. By Proposition 9, H is a subgroup. Then we may assume

$$\kappa_2(S) = |S|-1.$$

By Theorem 11, it would be enough to consider the case $|H| = 2$, say $H = \{0, x\}$. Put $N = \langle x \rangle$.

Decompose $S = S_0 \cup \cdots \cup S_j$ modulo N, where $|S_0 + H| \leq |S_1 + H| \leq \cdots \leq |S_j + H|$. We have $|S| + 1 = |S+H| = \sum\limits_{0 \leq i \leq j} |S_i + \{0, x\}|$.

Then $|S_i| = |N|$, for all $i \geq 1$. We have $j \geq 1$, since otherwise S would be an arithmetic progression. In particular N is finite. We have $|N+S| < |G|$, since otherwise $|S| \geq |G| - |N| + 1 \geq \frac{|G|+2}{2}$, a contradiction.

Now

$$\begin{aligned} |N| + |S| - 1 &= |N| + \kappa_2(S) \\ &\leq |S+N| = (j+1)|N| \\ &\leq |S| + |N| - 1, \end{aligned}$$

and hence N is a 2-fragment. ∎

Corollary 12 coincides with [[10],Theorem 4.6]. A special case of this result is Theorem 6.6 of [12]. As mentioned in [15], there was a misprint in this last statement. Indeed $|H| + |B| - 1$ should be replaced by $|H| + |B|$ in case (iii) of [Theorem 6.6, [12]].

The proof of Corollary 12 given here uses Proposition 9 and Theorem 11. These two results are not difficult and are proved in around 4 pages [with some possible simplifications if one forgets about very general results dealing with non abelian groups and abstract graphs] in [13].

Alternative proofs of Corollary 12 (with $|S| \leq |G|/2$ replacing $|S| \leq (|G|+1)/2$), using Kermperman's Theory were obtained by Grynkiewicz in [5] and Lev in [18]. In the present paper Corollary 12 will be one of pieces leading to a new proof of Kemperman's Theory.

4 Hyper-atoms

This section contains the new notion of a hyper-atom. Theorem 15 is one of the main results of this paper. As we shall see later it encodes most of the known results about the critical pair Theory.

4.1 Vosper subsets

Let $0 \in S$ be a generating subset of an abelian group G. We shall say that S is a *Vosper subset* if for all $X \subset G$ with $|X| \geq 2$, we have $|X+S| \geq \min(|G|-1, |X|+|S|)$.

Notice that S is a Vosper subset if and only if S is non 2–separable or if $\kappa_2(S) \geq |S|$.

Lemma 13 *Let S be a finite generating Vosper subset of an abelian group G such that $0 \in S$. Let $X \subset G$ be such that $|X| \geq |S| \geq 3$ and $|X+S| = |X|+|S|-1$. Then for every $y \in S$, we have $|X+(S \setminus \{y\})| \geq |X|+|S|-2$.*

Proof.

By the definition of a Vosper subset. We have $|X+S| \geq |G|-1$. Then one of the two possibilities:

Case 1. $|X+S| = |G|-1$.

Suppose that $|X+(S\setminus\{y\})| \leq |X|+|S|-3$ and take an element z of $(X+S)\setminus(X+(S\setminus\{y\}))$. We have $z-y \in X$. Also $(X \setminus \{z-y\})+S \subset ((X+S)\setminus\{z\})$. In particular we have by the definition of a Vosper subset, $|(X\setminus\{z-y\})+S| \geq \min(|G|-1, |X|-1+|S|) = |X|+|S|-1$. Clearly $X+S \supset ((X\setminus\{z-y\})+S)\cup\{z\}$. Hence $|X+S| \geq |X|+|S|$, a contradiction.

Case 2. $|X+S| = |G|$.

Suppose that $|X+(S\setminus\{y\})| \leq |X|+|S|-3$ and take a 2–subset R of $(X+S)\setminus(X+(S\setminus\{y\}))$. We have $R-y \subset X$. Also $(X\setminus(R-y))+S \subset (X+S)\setminus R$. In particular we have by the definition of a Vosper subset, $|(X\setminus(R-y))+S| \geq \min(|G|-1, |X|-2+|S|)$. We have $|X|=1$. Otherwise and since $X+S \supset ((X\setminus(R-y))+S)\cup R$, we have $|X+S| \geq |X|+|S|$, a contradiction. Then $|X|=1$. This forces that $|X|=|S|=3$, and hence $|G|=5$. Now by the Cauchy Davenport Theorem, $|X+(S\setminus\{y\})| \geq |X|+|S|-2$, a contradiction. ∎

4.2 Fragments in quotient groups

Lemma 14 *Let G be an abelian group and let S be a finite 2-separable generating subset containing 0. Let H be a subgroup which is a 2–fragment and let $\phi : G \mapsto G/H$ be the canonical morphism. Then*

$$\kappa_1(\phi(S)) = |\phi(S)|-1. \tag{4}$$

Let K be a subgroup which is a 1–fragment of $\phi(S)$. Then $\phi^{-1}(K)$ is a 2–fragment of S.

Proof.

Put $|\phi(S)| = u+1$. Since $|G| > |H+S|$, we have $\phi(S) \neq G/H$, and hence $\phi(S)$ is 1–separable.

Let $X \subset G/H$, be such that $X+\phi(S) \neq G/H$. Clearly $\phi^{-1}(X)+S \neq G$. Then $|\phi^{-1}(X)+S| \geq |\phi^{-1}(X)| + \kappa_1(S) = |\phi^{-1}(X)| + u|H|$.

It follows that $|X+\phi(S)||H| \geq |X||H| + u|H|$. Hence $\kappa_1(\phi(S)) \geq u = |\phi(S)|-1$. The reverse inequality is obvious and follows by (2). This proves (4).

Let K be a subgroup which is a 1–fragment of $\phi(S)$. Then $|K+\phi(S)| = |K| + u$. Then $|\phi^{-1}(K)+S| = |K||H| + u|H|$. In particular $|\phi^{-1}(K)$ is a 2–fragment. ∎

4.3 The fundamental property of hyper-atoms

Let S be a finite generating subset of an abelian group G such that $0 \in S$. Theorem 9 states that there is a 1–atom of S which is a subgroup. A subgroup with maximal cardinality which is a 1–fragment will be called a *hyper-atom*. This definition may adapted to non-abelian groups and even abstract graphs. As we shall see the hyper-atom is more closely related to the critical pair theory than the 2–atom.

Theorem 15 *Let S be a finite generating subset of an abelian group G such that $0 \in S$, $|S| \leq (|G|+1)/2$ and $\kappa_2(S) \leq |S|-1$. Let H be a hyper-atom of S. Then*

(i) $\phi(S)$ is either an arithmetic progression or a Vosper subset, where ϕ is the canonical morphism from G onto G/H.

(ii) Let $X \subset G/H$ be such that $|X+\phi(S)| = |X| + |\phi(S)| - 1$. Then for every $y \in \phi(S)$, $|X + (\phi(S) \setminus y)| \geq |X| + |\phi(S)| - 2$.

Proof.

Let us show that $2|\phi(S)| - 1 \leq \frac{|G|}{|H|}$. Clearly we may assume that G is finite.

Observe that $2|S+H| - 2|H| \leq 2|S| - 2 < |G|$. It follows, since$|S+H|$ is a multiple of $|H|$, that $2|S+H| \leq |G| + |H|$, and hence $2|\phi(S)| \leq \frac{|G|}{|H|} + 1$.

Suppose now that $\phi(S)$ is not a Vosper subset. By the definitions $\phi(S)$ is 2–separable and $\kappa_2(\phi(S)) \leq |\phi(S)| - 1$.

Observe that $\phi(S)$ can not have a 2-fragment M which is a subgroup. Otherwise by Lemmas 14 and 10, $\phi^{-1}(M)$ is a 2–fragment of S containing strictly H, contradicting the maximality of H. By Corollary 12, $\phi(S)$ is an arithmetic progression.

Now (ii) holds by Lemma 13 if $\phi(S)$ is a Vosper subset. It is also obvious if $\phi(S)$ is an arithmetic progression. ∎

Corollary 16 *Let S be a generating subset of a finite abelian group G such that $0 \in S$ and $|S| \leq \frac{|G|}{2}$, then one of the following conditions holds:*

(i) S is an arithmetic progression,

(ii) there is a subgroup $H \neq \{0\}$ such that $|H+A| < \min(|G|-1, |H|+|S|)$,

(iii) for any X such that $|X| \geq 2$, $|S+X| \geq \min(|G|-1, |S|+|X|)$.

Notice that the main aim of the authors of Corollary 16 was to give an application to sum free sets in finite abelian groups. The infinite case was irrelevant for this purpose. However the proof works if S is a finite subset of an abelian group if one uses [[10], Theorem 4.6] instead of Theorem 6.6 of [12]. Alternative proofs of Corollary 16 using Kermperman's Theory were obtained by Grynkiewicz in [5] and Lev in [18].

Theorem 15 implies clearly Corollary 16 with some improvements:

- The subgroup H in Theorem 15 is well described as a hyper-atom;
- We have also an equality $|H+S|-|H| = \kappa_1$, much precise than the inequality $|H+S| \leq |H|+|S|-1$. This equality will be needed later;
- The condition $|S| \leq \frac{|G|}{2}$ is relaxed to $|S| \leq \frac{|G|+1}{2}$.

Part (ii) of Theorem 15 is a critical pair result of a new type, that will be used later to prove Kemperman's structure Theorem.

5 Quasi-periodic decompositions

Theorem 17 *Let S, T be finite subsets of an abelian group G with $|S+T| = |S|+|T|-1$. Assume moreover that $S+T$ is aperiodic. Then one of the following holds:*

(i) S and T are K-quasi-periodic, for some nonzero subgroup K.

(ii) The pair $\{S,T\}$ is a strict elementary pair.

Proof.

The proof is by induction on $|S|+|T|$, the result being obvious for $|S|+|T|$ small. We may assume clearly that $0 \in S$. We may assume $\min(|S|,|T|) \geq 2$, since otherwise $\{S,T\}$ is a strict elementary pair and (ii) holds. Without loss of generality we may assume $2 \leq |S| \leq |T|$.

Claim 1 If $T \not\subset \langle S \rangle$, then the result holds.

Proof. Decompose $T = \bigcup_{i\in U} T_i$ modulo $\langle S \rangle$. By (3), $\kappa_1(S) \geq \frac{|S|}{2}$. Put $V = \{i \in U : |T_i+S| < |\langle S \rangle|\}$. By (1) we have

$$\begin{aligned} |T+S| &\geq (|U|-|V|)|\langle S \rangle| + \sum_{i\in V} |T_i+S| \qquad (5) \\ &\geq (|U|-|V|)|\langle S \rangle| + \sum_{i\in V} |T_i| + |V|\frac{|S|}{2} \geq |T| + |V|\frac{|S|}{2}. \end{aligned}$$

It follows that $|V| \leq 1$. But $|V| \geq 1$, since otherwise $T+S = T+S+\langle S\rangle$. Put $V = \{\omega\}$. By Kneser's Theorem $|T_\omega + S| \geq |T_\omega| + |S| - 1$. By (5) we have

$$|T| + |S| - 1 = |T+S| \quad \geq \quad (|U|-1)|\langle S\rangle| + |T_\omega| + |S| - 1$$

Therefore Then S and T are $\langle S\rangle$-quasi-periodic. ∎

By Claim 1, we may assume without loss of generality that

$$G = \langle S\rangle.$$

We may assume that S is not an arithmetic progression since otherwise T would be an arithmetic progression with the same difference, and (ii) would be satisfied.

Assume first $|G| - |T+S| = |T^S| < |T|$. Then G is finite. Observe that $T^S - S$ is aperiodic, otherwise by Lemma $T + S = (G \setminus (T^{S^{-S}})) + S$ would be periodic. By Kneser's Theorem $|T^S - S| = |T^S| + |S| - 1$. By the definition $(T^S - S) \cap T = \emptyset$. Therefore $|T^S - S| \leq |G| - |T| = |G| - |S+T| + |S+T| - |T| \leq |T^S| + |S| - 1$. Hence $T^S - S = G \setminus T$, and hence $T^{S^{-S}} = T$.

Then one of the following conditions holds by the induction hypothesis:

- S, T^S are N–quasi-periodic, for some non zero subgroup N. Therefore $T = G \setminus (T^S - S)$ is N–quasi-periodic. The result holds in this case.

- The pair $\{S, T^S\}$ is an elementary pair. Observe that S is not an arithmetic progression and hence (SP1) can not be satisfied for the pair $\{S, T^S\}$. Also $|T^S - S| = |G| - |T| \geq 2$ and then (SP3) can not be satisfied for the pair $\{S, T^S\}$.

  Then necessarily is $|T^S| = \min(|T^S|, |S|) = 1$. Let c denotes the unique element of $G \setminus (T+S)$. Then $c - T \subset G \setminus S$. But $|c-T| = |T| \geq |S+T| - |S| + 1 = |G| - |S|$. This shows that $c - T = G \setminus S$. Observe that T is aperiodic, since otherwise $T+S$ would be periodic.

  Case 1: $|(c-S) \cap T| \neq 1$ for every $c \in G$. In this case $\{T, S\}$ is a strict elementary pair and (ii) holds.

  Case 2: $|(c-S) \cap T| = 1$ for some $c \in G$. Put $c = x_1 + y_1$, where $x_1 \in T$ and $y_1 \in S$. Put $T' = T \setminus \{x_1\}$. Clearly $|T' + S| \leq |H| - 2 = |T'| + |S| - 1$. Let Q denotes the period of $T' + S$. By Kneser's Theorem 1, $|H| - 2 \geq |T' + S| \geq |T' + Q| + |S + Q| - |Q|$. This forces that $|Q| = 1$, since otherwise (observing that S is aperiodic) we have $|T| + |S| - 1 - |Q| = |H| - |Q| \geq |T' + S| \geq |T' + Q| + |S + Q| - |Q| \geq (|T| - 1) + (|S| + 1) - |Q|$, a contradiction.

  Therefore $|H| - 2 \geq |T' + S| \geq |T'| + |S| - 1 = |H| - 2$. Put $\{x_1, x_2\} = H \setminus (T' + S)$ and $d = x_2 - x_1$. Since $x_2 - d = x_1$, we have $x_2 \notin T' + S + d$. Since $T' + S$ is aperiodic, we have $|H| - 1 = |T' + S| + 1 \leq |T' + S + \{0, d\}| \leq |H| - 1$. Since $T' + S + \{0, d\}$ is aperiodic, we have Kneser's Theorem 1 $|(S + \{0, d\}) + T'| \geq |S + \{0, d\}| + |T| - 2$. It follows that $|S + \{0, d\}| \leq |S| + 1$. Hence S is $\langle d\rangle$–quasi-periodic. Similarly T is $\langle d\rangle$–quasi-periodic is $\langle d\rangle$–quasi-periodic. Then (i) holds in this case.

So we may assume that $|T| \leq |T^S|$.

By our assumptions $|T^S| = |G| - |T+S| \geq |T| \geq |S|$, we have

$$\begin{aligned} 3|S+T| &= 2|S+T|+|S|+|T|-1 \\ &\leq |G|-|S|+|G|-|T|+|S|+|T|-1 = 2|G|-1, \end{aligned}$$

In particular we have

$$|S+T| \leq \frac{2|G|-1}{3}. \tag{6}$$

Let H be a hyper-atom of S and let $\phi : G \mapsto G/H$ denotes the canonical morphism. Put $|\phi(S)| = u+1$ and $|\phi(T)| = t+1$. Put $q = \frac{|G|}{|H|}$.

Take a H–decomposition $S = \bigcup\limits_{0\leq i\leq u} S_i$ such that $|S_0| \geq \cdots \geq |S_u|$. By the definition we have $u|H| = |H+S|-|H| = \kappa_1 \leq |S|-1$. It follows that for all $u \geq j \geq 0$

$$|S_{u-j}| + \cdots + |S_u| \geq j|H|+1 \tag{7}$$

It follows that $|S_0| \geq \frac{|H|+1}{2}$. In particular S_0 generates H. We shall use this fact in the application of the isoperimetric inequality.

Take a H–decomposition $T = \bigcup\limits_{0\leq i\leq t} T_i$.

By (4), $\kappa_1(\phi(S)) = |\phi(S)|-1 = u$. Put $\ell = \min(q-t-1, u)$.

By Proposition 6 applied to $\phi(S)$ and $\phi(T)$, there is a subset $J \subset [0,t]$ with cardinality ℓ and a family $\{mi; i \in J\}$ of integers in $[1,u]$ such that $T+S$ contains the H–decomposition $(\bigcup\limits_{0\leq i\leq t} T_i + S_0) \cup (\bigcup\limits_{i\in J} T_i + S_{mi})$.

Put $R = (S+T) \setminus ((\bigcup_{i\in J} T_i + S_{mi} + H) \cup (\bigcup_{0\leq i\leq t} T_i + H))$.

We shall choose such a J in order to maximize $|J \cap P|$. We shall write $E_i = (S+T) \cap (T_i+H)$, for every $i \in [0,t]$. Also we write $E_{mi} = (S+T) \cap (T_i + S_{mi} + H)$, for every $i \in J$.

We put also $W = \{i \in [0,t] : |E_i| < |H|\}$, and $P = [0,t] \setminus W$.

Since $|T| \geq |S|$ we have $|T+H| \geq |S| > \kappa_2(S) = u|H|$. It follows that $t+1 = |\phi(T)| \geq u+1$. Then $t+1-|J| > 0$. In particular $I \neq \emptyset$, where $I = [0,t] \setminus J$.

Let X be a subset of I and let Y be a subset of J. We have

$$\begin{aligned} |S+T|-|R| &\geq \sum_{i\in X\cup Y} |E_i| + \sum_{i\in I\setminus X\cup J\setminus Y} |T_i+S_0| + \sum_{i\in J\setminus Y} |T_i+S_{mi}| + \sum_{i\in Y} |E_{mi}| \\ &\geq \sum_{i\in X\cup Y} |E_i| + \sum_{i\in I\setminus X\cup J\setminus Y} |T_i| + (u-|Y|)|S_0| + \sum_{i\in Y} |E_{mi}| \qquad (8) \\ &\geq \sum_{i\in X\cup Y} |E_i| + \sum_{i\in I\setminus X\cup J\setminus Y} |T_i| + (u-|Y|)|S_0| + |Y||S_u| \qquad (9) \end{aligned}$$

Put $F = \{i \in I \cap P : (T_i+S) \cap (\bigcup_{i\in W} T_i + H) \neq \emptyset\}$.

We shall use the following obvious facts: For all $i \in W$, we have by (3), $|E_i| \geq |T_i + S_0| \geq |T_i| + \kappa_1(S_0) \geq |T_i| + \frac{|S_0|}{2}$. For every $i \in F$, $T_i + S_{ri} \subset T_j + H$ for some $1 \leq ri \leq u$ and some $j \in W$. Hence we have $|T_i| + |S_u| \leq |T_i| + |S_{ri}| \leq |H| = |E_i|$, by Lemma 3.

Let U be a subset of $W \cap J$. Put $X = I$ and $Y = U$. By (9), we have

$$\begin{aligned} |S+T| - |R| &\geq \sum_{i \in U \cup (W \cap I) \cup (P \cap I)} |E_i| + \sum_{i \in J \setminus U} |T_i| + (u - |U|)|S_0| + |U||S_u| && (10) \\ &\geq \sum_{i \in (P \cap I) \setminus F} |T_i| + \sum_{i \in F} (|T_i| + |S_u|) + \sum_{i \in (W \cap I) \cup U} (|T_i| + \frac{|S_0|}{2}) + |J \setminus U||S_0| + |U||S_u| \\ &\geq |T| + |J \setminus U||S_0| + (|U| + |F|)|S_u| + |(W \cap I) \cup U| \frac{|S_0|}{2}. && (11) \end{aligned}$$

Claim 2 $q \geq |\phi(S)| + |\phi(T)| - 1$, and hence $\ell = u$.

Proof. The proof is by contradiction. Suppose that $q < |\phi(S)| + |\phi(T)| - 1$.

Assume first $u \geq 2$. By Lemma 3, the are two distinct values of the pair (s, t) such that $T_s + S_t \subset E_{mi}$, for every $i \in J$. In particular $|E_{mi}| \geq |S_{u-1}|$, for every $i \in J$. Also $|E_i| \geq |S_0|$, for every $i \in [0, t]$.

Observe that $2t > t + u \geq q$. We have using (7)

$2|S_0| \geq |S_0| + |S_{u-1}| \geq \frac{2}{3}(|S_u| + |S_{u-1}| + |S_{u-2}) > \frac{4|H|}{3}$. By (9), applied with $X = I$ and $Y = J$, we have

$$\begin{aligned} |S+T| &\geq \sum_{0 \leq i \leq t} |S_0| + \sum_{i \in J} |S_{u-1}| = (t+1)|S_0| + (q-t-1)|S_{u-1}| \\ &= (2t+2-q)|S_0| + (q-t-1)(|S_0| + |S_{u-1}|) \\ &> (2t+2-q)\frac{2|H|}{3} + \frac{4|H|(q-t-1)}{3} = \frac{2|G|}{3}, \end{aligned}$$

contradicting (6).

Assume now $u = 1$. From the inequality $|T + S| \leq |T| + |S| - 1$, we see that $\kappa_1(S) \leq |S| - 1$. Therefore we have by (6), $\frac{2|G|}{3} > |T + S| \geq |T| + \kappa_1(S) \geq |S| + |H| > 2|H|$, and hence

$$q \geq 4.$$

We have $(t+1) + (u+1) - 1 < |\phi(S+T)| \leq q$. Then $t + 1 = q$. Hence $\ell = |J| = 0$. We have $|W| \geq 1$, since otherwise $G = T + H \subset S + T$. We have $|W| \leq 3$, by (11) applied with $U = \emptyset$. Therefore $|P| \geq t + 1 - 3 \geq 4 - 3 = 1$. There is clearly $i \in P$ with $T_i + S_1 \subset T_j + H$ for some $j \in W$, and hence $|F| \geq 1$. By (11) applied with $U = \emptyset$, $|T + S| \geq |T| + |W|\frac{|S_0|}{2} + |S_1|$, and hence $|W| \leq 1$. It follows that $|S + T| \geq |G| - |H| = |G| - \frac{|G|}{q} \geq \frac{3|G|}{4}$, contradicting (6). ∎

We must have $R = \emptyset$, since otherwise by (11) applied with $U = \emptyset$, $|S + T| - |R| \geq |S + T| - |S_u||\phi(R)| \geq |T| + u|S_0| + |S_u| \geq |T| + |S|$, a contradiction. In particular

$$|\phi(S+T)| = |\phi(S)| + |\phi(T)| - 1. \tag{12}$$

Claim 3. $J \cap P \neq \emptyset$.

Proof. Suppose the contrary and take $k \in J \cap W$. Put $U = \{k\}$. By (11),

$$|S| + |T| > |S+T| \quad \geq \quad |T| + (u-1)|S_0| + |S_u| + (|W \cap I| + 1)\frac{|S_0|}{2}.$$

It follows that $I \subset P$. Since S generates G, we have $|\bigcup_{i\in I} T_i + H + S| > |\bigcup_{i\in I} T_i + H|$.

We must have $(\bigcup_{i\in I} T_i + H + S) \cap (\bigcup_{i\in J} E_{mi} + H) = \emptyset$, since otherwise by replacing a suitable element of J with some $p \in I$, we may increase strictly $|J \cap P|$, observing that $I \subset P$.

By (12), there are $i \in I$, $j \in J$ and $p \in [1, u]$ such that $T_i + S_p$ is congruent $T_j + S_{mj}$. It follows that $F \neq \emptyset$.

By (11) applied with $U = \emptyset$,

$$|S+T| \quad \geq \quad |T| + u|S_0| + |S_u| \geq |T| + |S|,$$

a contradiction proving the claim. ∎

Take $r \in J$ with $|E_r| = |H|$. Such an r exists by Claim 3.

Claim 4 $T_i + H + S_j = T_i + S_j$, for all $0 \leq j \leq u-1$.

Proof. By Lemma 3, it would be enough to show the following:

$$|T_k| + |S_{u-1}| > |H|, \tag{13}$$

for every $k \in [0, t]$. Suppose the contrary.

Notice that $|E_{mr}| \geq \max(|T_r|, |S_u|)$ and that $|E_k| \geq |S_0|$. Also $|T_k| + |S_{u-1}| \leq |H| = |E_{mr}|$ by our choose of r. We shall use these inequalities and (8) with $X = \{k, r\} \cap I$ and $Y = \{k, r\} \cap J$.

By (8) we have for $k \neq r$,

$$\begin{aligned} |S+T| &\geq |T| - |T_k| - |T_r| + (u - |X|)|S_0| + |T_k| + |S_{u-1}| + |S_0| + |T_r| + |Y||S_u| \\ &\geq |T| + (u-1)|S_0| + |S_{u-1}| + |S_u| \geq |T| + |S|, \end{aligned}$$

leading a contradiction. If $k = r$ the contradiction comes more easily. ∎

Since $|S+T| < |G|$, we must have by Lemma 3,

$$2|S| \leq |S| + |T| \leq |G|.$$

Now by (12) and Theorem 15, $|\phi(T + (S \setminus S_u))| \geq t + u$. Take a subset Ω of $\phi(T + (S \setminus S_u))$ with $|\Omega| = u + t$. By (12), $\phi(T+S) = \Omega \cup \{\omega\}$, for some $\omega \in G/H$. By Claim 4, $(\phi^{-1}(\Omega)) \cap (T+S)$ is H–periodic. Necessarily there is s such that $|E_{ms}| < |H|$. Then by Claim 4 $E_{ms} = T_s + S_u$.

Since $T+S$ is aperiodic, and since $(T+S)\setminus E_{ms}$ is H–periodic, we have that T_s+S_u is aperiodic. By Kneser's Theorem, $|T_s+S_u|\geq |T_s|+|S_u|-1$. Now we have

$$\begin{aligned}|S|+|T|-1 &= |S+T|\\ &= |(\psi^{-1}(\Omega))\cap(T+S)|+|E_{ms}|\\ &\geq (t+u)|H|+|E_{ms}|\\ &\geq (t+u)|H|+|T_s|+|S_u|-1\geq |T|+|S|-1.\end{aligned}$$

Therefore $|T|=t|H|+|T_s|$ and $|S|=u|H|+|S_u|$. Hence T and S are H–periodic. ▮

Proof of Theorem 2:

The implication (II) ⇒ (I) is quite easy. Let us prove the implication (I)⇒(II). Suppose that (I) holds.

Assume first that $A+B$ is aperiodic. Note that $(\emptyset,A)$ and $(\emptyset,B)$ are G-quasi-periodic decompositions. Take a subgroup H with minimal cardinality $|H|\geq 2$ for which there are H–quasi-periodic decompositions $A=A_0\cup A_1$ and $B=B_0\cup B_1$. Let $\phi: G\mapsto G/H$ be the canonical morphism. Take $a_1\in A_1$ and $b_1\in B_1$.

Notice that A_1 and B_1 have no P-quasi periods for some $2\leq |P|<|H|$, otherwise $|H|$ would be not minimal. By Theorem 17, the pair $\{A_1,B_1\}$ is an elementary pair. Since $A+B$ is aperiodic, $\phi(a_1)+\phi(b_1)$ has a unique expression.

Assume now that $A+B$ is periodic.

Let H be a period of $A+B$ with a prime order and let $\phi: G\mapsto G/H$ is the canonical morphism.

Let C denotes the set of elements of $A+B$ having a unique expression. Clearly $c\in C$. To each $x\in C$, choose $a_x\in A$ and $b_x\in B$ such that $x=a_x+b_x$. Put $A_x=A\cap(a_x+H)$.

Observe that $\phi(c)=\phi(a_c)+\phi(b_c)$ has a unique expression. Hence by Scherck's Theorem 4, $|\phi(A)+\phi(B)|\geq|\phi(A)|+|\phi(B)|-1$. We must have $|\phi(A)+\phi(B)|=|\phi(A)|+|\phi(B)|-1$, since otherwise $|A+B|=|\phi(A+B)||H|=|A|+|B|$. By Lemma 3, we have

$$|A_x|+|B_x|\leq |H|+1.$$

Observe that $|A|+|B|-1=|A+B|=|\phi(A+B)||H|=|A+H|+|B+H|-|H|$. It follows that the trace of A (resp. B)on any coset $\neq A_x+H$ (resp. $\neq B_x+H$) has cardinality $=|H|$. It follows that $A\setminus A_x$ and $B\setminus B_x$ are H-periodic sets.

If $|C|=1$, then $\{A_c,B_c\}$ is an elementary pair. So we may assume that $|C|\geq 2$. We may assume that $|A_c|\geq 2$, since otherwise $\{A_c,B_c\}$ is an elementary pair (verifying SP2). Assume first that $|A_c|=2$, say $A_c=\{a,a+d\}$. Then $|B_c|=|H|-1$ and hence B_c is an arithmetic progression of difference d (recall that $|H|$ is a prime). It follows that $\{A_c,B_c\}$ is an elementary pair (verifying SP1). So we may assume that $|A_c|\geq 3$.

Suppose that there is $v\in C\backslash\{c\}$, with $A_v\neq A_c$ or $B_v\neq B_c$. Without loss of generality we may take $A_v\neq A_c$. Since $A\backslash A_v$ is H–periodic, we have $|A_c|=|H|$. Then $|B_c|=|H|+1-|A_c|=1$. It follows that $\{A_c,B_c\}$ is an elementary pair.

Therefore there is $v\in C\setminus\{c\}$, with $A_v=A_c$ and $B_v=B_c$. Put $c=c_1+d_1$ and $v=c_2+d_2$, with $c_1,c_2\in A$ and $d_1,d_2\in B$. Now we have $|B_c|\geq|A_c|\geq 3$. If $|H|=5$, then A_c,B_c, have cardinality $= 3$, and hence they are arithmetic progressions. The unique expressibility of c implies that A_c, B_c have the same difference. It follows that $\{A_c, B_c\}$ is an elementary pair (verifying SP1). So we may assume that $|H| \geq 7$. Therefore $2|B_c| \geq |B_c|+|A_c| = |H|+1 \geq 8$.

Put $B' = B_c \setminus \{c_1, d_1\}$. We have clearly $|H| - 2 = |A'| + |B_c| - 1 \geq |B' + A_c|$. By Vosper's Theorem A_c, B' are arithmetic progressions with a same difference say d. Since $|(B_c \setminus \{c_i\}) + A_c| \leq |B_c \setminus \{c_i\}| + |A_c| - 1$, we must have that $B_c \setminus \{c_i\}$ is an arithmetic progression with difference $= d$ and extremity c_i. This shows that $\{A_c, B_c\}$ is an elementary pair (verifying SP1). theorem is proved in this case.

∎

6 Appendix: A short proof of Scherck's Theorem

Proof of Theorem 4:

We start by a special.

Claim For any two finite subset A, B such that $A \cap (-B) = \{0\}$, we have $|A+B| \geq |A|+|B|-1$.

The proof is by induction on $|B|$, the result being obvious for $|B| = 1$.

Since $0 \in A \cap B$, we have $|A + B| \geq |A \cup B| = |A| + |B| - |A \cap B|$. Therefore we may assume that there is $b \in A \cap B$, with $b \neq 0$.

Put $B' = B \cap (B - b)$. We have $B - b \neq B$, since otherwise we would have $b \in A \cap -B$, a contradiction. Hence $0 \in B'$ and $|B'| < |B|$.

Put $A' = A \cup A + b$. We have $A' \cap -B' = (A \cap -B) \cap (-B + b) \cup A + b \cap (-B + b) \cap (-B) = \{0\}$.

The result follows by induction.

We may put $c = c_1 + c_2$, where $c_1 \in X$ and $c_2 \in Y$. Put $A = X - c_1$ and $B = Y - c_2$. The result follows by the Claim. ∎

References

[1] E. Balandraud, Un nouveau point de vue isopérimetrique appliqué au théorème de Kneser, *Preprint*, december 2005.

[2] A. Cauchy, Recherches sur les nombres, *J. Ecole polytechnique* 9(1813), 99-116.

[3] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* 10(1935), 30–32.

[4] A. Geroldinger, F. Halter-Koch, Non-unique factorizations. Algebraic, combinatorial and analytic theory. Pure and Applied Mathematics (Boca Raton), 278. Chapman & Hall/CRC, Boca Raton, FL, 2006. xxii+700 pp.

[5] D. Grynkiewicz, Quasi-periodic decompositions and the Kemperman's structure theorem, European J. Combin. 26 (2005), no. 5, 559–575.

[6] D. Grynkiewicz, A step beyond Kemperman's structure Theorem, Preprint May 2006.

[7] Y.O. Hamidoune, Sur les atomes d'un graphe orienté, *C.R. Acad. Sc. Paris A* 284 (1977), 1253–1256.

[8] Y.O. Hamidoune, Quelques problèmes de connexité dans les graphes orientés, *J. Comb. Theory* B 30 (1981), 1-10.

[9] Y.O. Hamidoune, On the connectivity of Cayley digraphs, *Europ. J. Combinatorics*, 5 (1984), 309-312.

[10] Y.O. Hamidoune, Subsets with small sums in abelian groups I: The Vosper property. European J. Combin. 18 (1997), no. 5, 541–556.

[11] Y.O. Hamidoune, An isoperimetric method in additive theory. *J. Algebra* 179 (1996), no. 2, 622–630.

[12] Y.O. Hamidoune, Some results in Additive number Theory I: The critical pair Theory, Acta Arith. 96, no. 2(2000), 97-119.

[13] Y.O. Hamidoune, Some additive applications of the isopermetric approach, http://arxiv.org/abs/math./07060635.

[14] Y.O. Hamidoune, The global isoperimetric methodology applied to Kneser's Theorem, Preprint August-2007.

[15] Y. O. Hamidoune , A. Plagne. A new critical pair theorem applied to sum-free sets. *Comment. Math. Helv.* 79 (2004), no. 1, 183–207.

[16] Y. O. Hamidoune, Ø. J. Rødseth, An inverse theorem modulo p, *Acta Arithmetica* 92 (2000)251–262.

[17] J. H. B. Kemperman, On small sumsets in Abelian groups, *Acta Math.* 103 (1960), 66–88.

[18] V. F. Lev, Critical pairs in abelian groups and Kemperman's structure theorem. *Int. J. Number Theory* 2 (2006), no. 3, 379–396.

[19] M. B. Nathanson, *Additive Number Theory. Inverse problems and the geometry of sumsets*, Grad. Texts in Math. 165, Springer, 1996.

[20] P. Scherk, L.Moser, Advanced Problems and Solutions: Solutions: 4466,*Amer. Math. Monthly* 62 (1955), no. 1, 46–47.

[21] T. Tao, V.H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics 105 (2006), Cambridge University Press.